Notes on Ribet's Converse to Herbrand

Chandrashekhar Khare

1. Statement of the theorem

Let p be an odd prime. It is called irregular if and only if p divides the class number of $\mathbf{Q}(\mu_p)$. By Kummer's criterion this happens if and only if p divides the numerator of the kth Bernoulli number B_k for an even k between 2 and $p-3$ (note that the denominator is prime to p because of the von-Staudt-Clausen theorem). Recall that the Bernoulli numbers B_n are defined by:

$$\frac{t}{e^t-1}+\frac{t}{2}-1=\Sigma_{n\geq 2}\frac{B_n}{n!}t^n.$$

The first few Bernoulli numbers are

$$B_4=\frac{-1}{30}, B_6=\frac{1}{42}, B_8=\frac{-1}{30}, B_{10}=\frac{5}{66}, B_{12}=\frac{-691}{2730}.$$

Let A be the ideal class group of $\mathbf{Q}(\mu_p)$ and let C be the $\mathbf{F}_p$-vector space A/A^p. This has an action of the Galois group $\Delta := Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) \equiv (\mathbf{Z}/p\mathbf{Z})^*$. We define the mod p cyclotomic character $\chi : \Delta \to (\mathbf{Z}/p\mathbf{Z})^*$ by $g.\zeta = \zeta^{\chi(g)}$. Note that χ generates the character group of Δ with the characters taking values in $\overline{\mathbf{F}}_p^*$.

As Δ has order prime to p we have a canonical decomposition of C as

$$C=\oplus_{i \pmod{p-1}} C(\chi^i)$$

where $C(\chi^i)$ is the χ^i-isotypical component of C as a Δ-module. Note that $C(\chi^i)=e_{\chi^i}C$ where

$$e_{\chi^i}=\frac{1}{p-1}\Sigma_{g\in\Delta}\chi^{-i}(g)g.$$

The main theorem proven by Ribet in [R] is:

Theorem 1 *Let k be an even integer, $2 \leq k \leq p-3$. Then p divides the numerator of B_k if and only if $C(\chi^{1-k}) \neq 0$.*

It was known classically by Herbrand, refining Stickelberger's theorem, that if $C(\chi^{1-k}) \neq 0$, then p divides (numerator of) B_k (Section 3 of Chapter 1 of [L]). The converse was also well-known assuming Vandiver's conjecture

that $\mathbf{Q}(\mu_p)^+$ has class number prime to p. The theorem is also a consequence of the Main Conjecture of Iwasawa theory which was proved for abelian number fields by Mazur-Wiles ([MW]). The proof of Ribet, and its reinterpretation and extension in [W], was a significant clue for the work of Mazur-Wiles. Now its possible to give technically simpler proofs of this result using the important technique of Euler systems developed by Kolyvagin (see Rubin's appendix in [L]). But the proof of Ribet is still valuable as it *explicitly* constructs abelian, unramified extensions of exponent p of $\mathbf{Q}(\mu_p)$ with controlled behaviour.

Note that by class field theory we have an isomorphism via the Artin symbol, that we denote by Art, of C with the maximal unramified abelian p-extension E of $\mathbf{Q}(\mu_p)$ (note that the p-torsion of A can be identified with C as a Δ-module). The abelian Galois group $H := Gal(E/\mathbf{Q}(\mu_p))$ has an action of the group Δ by conjugation, that also acts on C as seen above. The Artin reciprocity map is equivariant for the action of Δ. Namely we have

$$Art : g.\mathfrak{c} \in C \rightarrow gArt(\mathfrak{c})g^{-1} \in H.$$

Thus under the hypothesis that p divides B_k $(2 \leq k \leq p-3)$ to construct a non-trivial element in $C(\chi^{1-k})$ it is enough to construct an unramified abelian p-extension $E/\mathbf{Q}(\mu_p)$ (so $Gal(E/\mathbf{Q}(\mu_p))$ is a $\mathbf{Z}/p\mathbf{Z}$ vector space) such that Δ acts on it via χ^{1-k}.

We easily see that then $Gal(E/\mathbf{Q})$ is the semi-direct product of $(\mathbf{Z}/p\mathbf{Z})^r$ (for some positive integer r) by $\mathbf{Z}/p\mathbf{Z}^*$, with the action given by $g.a = \chi^{1-k}(g)a$, $g \in \Delta, a \in Gal(E/\mathbf{Q}(\mu_p))$.

We claim that Theorem 1 follows from:

Theorem 2 *Suppose $p|B_k$. Then there is a representation*

$$\rho : G_{\mathbf{Q}} \rightarrow GL_2(\mathbf{F}),$$

where $\mathbf{F}$ is a finite extension of $\mathbf{F}_p$ with the properties:

(i) ρ is unramified at all primes different from p.

(ii) ρ is a reducible non-semisimple representation of the form

$$\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$$

with the $*$ non-trivial: another way to say this is the order of the image of ρ is divisible by p.

(iii) Let D be a decomposition group of p in $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$. Then the order of $\rho(D)$ is prime to p: namely the representation ρ when restricted to D is semisimple.

We justify the claim:

If we define E' to be the fixed field of the kernel of ρ, then the fixed field $\mathbf{Q}(\mu_p)^{\otimes(k-1)}$ of the subgroup consisting of matrices of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

is a subfield of $\mathbf{Q}(\mu_p)$ (of order $\frac{(p-1)}{(p-1,k-1)}$), and $Gal(\mathbf{Q}(\mu_p)^{\otimes(k-1)}/\mathbf{Q})$, which is the quotient through which χ^{1-k} factors, acts on $H' := Gal(E/\mathbf{Q}(\mu_p)^{\otimes(k-1)})$ by χ^{1-k}. Because of (ii), H' is a group of $(p, \cdots, p)$ type. The extension $E/\mathbf{Q}(\mu_p)^{\otimes(k-1)}$ is unramified as (i) implies that it is unramified outside p, while (iii) implies that the primes above p split in the extension $E/\mathbf{Q}(\mu_p)^{\otimes(k-1)}$ as this is an extension of $(p, \cdots, p)$ type. Now if we define E to be the compositum of E' and $\mathbf{Q}(\mu_p)$, then as $\mathbf{Q}(\mu_p)$ and E' are linearly disjoint extensions of $\mathbf{Q}(\mu_p)^{\otimes(k-1)}$, the extension $E/\mathbf{Q}(\mu_p)$ has the desired properties.

2. Strategy of proof

It remains only to prove Theorem 2! The existence of the representation ρ is subtle as one wants a two dimensional mod p representation of the Galois group of $\mathbf{Q}$ that is *not* semisimple while its restriction to D is semisimple.

Ribet uses the 2 dimensional mod p representations that arise from the reduction mod p of the p-adic representation attached to cusp forms f that are eigenvectors for Hecke operators. These generally tend to be irreducible unless f is *congruent* to an Eisenstein series mod p.

In particular, consider the Eisenstein series

$$E_k = -B_k/2k + \Sigma_n \sigma_{k-1}(n) q^n,$$

where $q = e^{2\pi i z}$. As $p|B_k$, E_k mod p "looks like" a cusp form, as mod p it vanishes at infinity. In fact there is a cuspidal eigenform $f \in S_k(SL_2(\mathbf{Z}))$ that is "congruent" to E_k mod p. Using the form f, Ribet constructs the representation ρ. The properties (i) and (ii) are not hard to prove, but (iii) requires very delicate results from algebraic geometry ([Ra]).

In fact when Ribet worked out his results enough was not known about mod p representations coming from cuspforms of weight bigger than 2, and he was forced to work at weight 2 using (by now) well-known principles that "mod p everything is weight 2". But now because of recent results proven by Faltings, Jordan ([FJ]), and the theory of Fontaine-Laffaille ([FL]) it seems possible to work directly in higher weights k ($k \leq p-3$). We will give

indications of how (i) and (ii) are proved below, and hand wave our way through (iii)!

3. The proof

3.1 Galois representations attached to cuspforms

Let $N \geq 1$, $k \geq 2$ be integers, $\epsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ a character. Then we consider the space of $S_k(\Gamma_0(N), \epsilon) \subset S_k(\Gamma_1(N))$ of cuspforms of weight k for the congruence subgroup

$$\Gamma_0(N) = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbf{Z}) \mid c \equiv 0 \ (N),$$

with character ϵ. These are holomorphic functions f on the upper half-plane $\mathcal{H} = \{z \in \mathbf{C} | im(z) > 0\}$ such that

$$f(\frac{az+b}{cz+d}) = \epsilon(d)(cz+d)^k f(z)$$

for

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(N),$$

with the condition that f vanishes at all cusps. This latter condition simply means that $f(\frac{az+b}{cz+d})$ tends to 0 whenever $im(z) \to \infty$ for any matrix

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbf{Z}).$$

There is another useful algebraic way of looking at cuspforms f of weight 2. Consider the open Riemann surface $\mathcal{H}/\Gamma_1(N)$. This can be viewed as an affine curve and one can compactify it to get a projective curve $X_1(N)$. We can view this sitting in $\mathbf{P}^n$ for some n, and it is a theorem that the equations which define this curve can be chosen to be stable under the action of the Galois group of $\mathbf{Q}$. A remark for the experts: we will implicitly work with Shimura's canonical model for these modular curves (and denote them by $X_1(N)$) over $\mathbf{Q}$. As a Riemann surface we have the uniformisation

$$\pi : \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}) \to X_1(N).$$

If we consider a holomorphic differential ω on the curve $X_1(N)$ its pull-back $\pi^*(\omega)$ can be written as $f(z)dz$ (on the curve $X_1(N)$, ω looks like that only

locally), and as $\alpha^*(dz) = d(\alpha(z)) = (cz+d)^{-2}dz$ with $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, we see that f has the "right symmetries". As $dz" = "dq/q$ we see that as ω is a homolomorphic differential on $X_1(N)$, f is forced to be a cuspform. Thus we have an interpretation of the space of cuspforms of weight 2 as the space of holomorphic differentials etc, an interpretation that will be useful later. For higher weights there is also a similar interpretation except that we have to use differentials with values in non-trivial coefficient systems.

As the element

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$$

we can develop f in a Fourier series

$$f = \Sigma_n a_n(f) q^n.$$

We have an action of Hecke operators T_n on the space $S_k(\Gamma_0(N), \epsilon)$: explicitly for most primes r the action of T_r is given by

$$f|T_r = \Sigma_n a_{nr}(f) q^n + \epsilon(r) r^{k-1} \Sigma_n a_n(f) q^{nr}.$$

The Hecke operators generate a commutative algebra that we shall denote by $h_1(N)$. Inside the space of cusp forms we also have the lattice of cusp forms with Fourier coefficients in $\mathbf{Z}[\epsilon]$: these are preserved by the Hecke operators, and the Hecke algebra acting on them is a free $\mathbf{Z}$-module of finite rank.

Consider $f \in S_k(\Gamma_0(N), \epsilon)$ which is an eigenform for almost all T_r's where r is a prime. One can then show that the Fourier expansion of f has coefficients which lie in a number field. Further for any automorphism $\sigma \in G_{\mathbf{Q}}$, $f^\sigma := \Sigma_n a_n(f)^\sigma q^n$ is in $S_k(\Gamma_0(N), \epsilon^\sigma)$. This is not evident, but follows from a cohomological interpretation of cusp forms. Be that as it may, the big result here is that associated to f, and any prime ℓ there is a representation

$$\rho_f : G_{\mathbf{Q}} \to GL_2(E),$$

where E is a finite extension of $\mathbf{Q}_\ell$, that is characterised upto semisimplification by:

1. ρ_f is unramified at almost all primes r
2. For almost all primes r the characteristic polynomial of $\rho_f(Frob_r)$ is $x^2 - a_r(f)x + \epsilon(r)r^{k-1}$

Note that amongst the excluded primes in the phrase "for almost all primes" is the prime ℓ. This result is due to Eichler, Shimura and Deligne.

It is not clear if the representation ρ_f is semisimple. But in fact we have:

Theorem 3 *The representation ρ_f is absolutely irreducible.*

Proof. We will prove this only for even weights k, though it is true even for odd weights. This follows from the Ramanujan bounds, proven by Deligne, that for an eigencuspform

$$|a_r(f)| \leq 2r^{(k-1)/2},$$

for almost all primes r. Now if the representation were reducible we would have that the semisimplification would be the sum of two ℓ-adic characters $\chi^r\epsilon_1$ and $\chi^s\epsilon_2$ for integers r, s (by results about Hecke characters in [S]), with χ the ℓ-adic cyclotomic character of $G_{\mathbf{Q}}$ giving the action on roots of unity whose order is some power of ℓ, and ϵ_i finite order characters of $G_{\mathbf{Q}}$. The cyclotomic character χ has the property that for all primes $t \neq \ell$, $\chi(Frob_t) = t$. Comparing determinant characters for ρ_f we deduce that $r + s = k - 1$ and r and s are unequal as k is even: this contradicts the Ramanujan bounds.

The representation ρ_f is continuous with respect to the profinite topology on $G_{\mathbf{Q}}$ (the open subgroups are the subgroups of finite index: the group is totally disconnected and compact), and the ℓ-adic topology on $GL_2(E)$. As the group $GL_2(\mathcal{O}_E)$, with $\mathcal{O}_E$ the ring of integers of E, is open, the inverse image of it under ρ_f is a subgroup H of finite index of $G_{\mathbf{Q}}$: thus H stabilises a lattice L' in E^2 under the action of ρ_f. If we let L be the sum of the translates of L' under the coset representaives of H in $G_{\mathbf{Q}}$, we see that $G_{\mathbf{Q}}$ stabilises L. With respect to a basis of $L = \mathcal{O}_E e_1 + \mathcal{O}_E e_2$, the representation takes values in $GL_2(\mathcal{O}_E)$. We can reduce this integral model of the representation modulo the maximal ideal of $\mathcal{O}_E$, to get a representation $\overline{\rho}_f : G_{\mathbf{Q}} \to GL_2(\mathbf{F})$, where $\mathbf{F}$ is a finite field of characteristic ℓ.

Note that there are many choices of lattices L which $G_{\mathbf{Q}}$ stabilises, and thus $\overline{\rho}_f$ depends on the choice of L. But we have the theorem of Brauer-Nesbitt:

Theorem 4 *The semisimplification $\overline{\rho}_f^{ss}$ of the reduction mod l of ρ_f is well-defined, i.e., does not depend on the choice of lattice.*

Now choose ℓ to be the prime p that we are interested in. Assume now that ρ_f is such that its reduction w.r.t. some lattice L is reducible. Then Theorem 4 implies that its reduction w.r.t. any lattice is reducible. The following proposition is crucial to Ribet's work:

Proposition 1 *Assume ρ_f is such that its reduction with respect to some lattice $L \subset E^2$ (and hence all lattices) stabilised by $G_{\mathbf{Q}}$ is reducible with semisimplification isomorphic to $\phi_1 \oplus \phi_2$, for ϕ_i characters of $G_{\mathbf{Q}} \to \overline{\mathbf{F}_p^*}$. Then there is a lattice L' such that the reduction of ρ_f with respect to L' is not semisimple and of the form $\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$, for a specific choice of ϕ_1 and ϕ_2.*

Proof. For the proof of this the crucial ingredient is Theorem 3: ρ_f is irreducible.

Let π be a uniformiser of $\mathcal{O}_E$. Note the conjugation formula

$$P \begin{pmatrix} a & \pi b \\ c & d \end{pmatrix} P^{-1} = \begin{pmatrix} a & b \\ \pi c & d \end{pmatrix},$$

where $P := \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$. Because of this we may assume that the reduction of a chosen integral model of the representation is of the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$.

We first claim that we can choose a $\rho_f(G_{\mathbf{Q}})$-lattice L so that the mod p representation is of the form $\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$, rather than $\begin{pmatrix} \phi_2 & * \\ 0 & \phi_1 \end{pmatrix}$. This follows from the conjugation formula

$$Q_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} Q_k^{-1} = \begin{pmatrix} d & -c/\pi^k \\ -\pi^k b & a \end{pmatrix},$$

where $Q_k := \begin{pmatrix} 0 & 1 \\ -\pi^k & 0 \end{pmatrix}$. Choose k to be the lowest power of π which divides all the lower left-corner entries of $\rho_f(g)$ for all $g \in G_{\mathbf{Q}}$ in its matricial representation with respect to some lattice. As ρ_f is irreducible k is a non-negative integer, and because of the above assumption, k is positive. From this the claim follows. Now we *fix* a lattice L so that the reduction of ρ_f with respect to it is of the form $\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$.

For the sake of contradiction let us assume that the reduction of ρ_f with respect to all $G_{\mathbf{Q}}$-stable lattices is semisimple, i.e., is of the form $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$, where the $*$ are 1-dimensional characters. Choosing the integral model of ρ_f given by L, if we conjugate $\rho_f(G_{\mathbf{Q}}) \subset GL_2(\mathcal{O}_E)$ by a matrix M such that $M\rho_f(G_{\mathbf{Q}})M^{-1} \subset GL_2(\mathcal{O}_E)$ then its mod p reduction is again reducible and semisimple.

To get a contradiction we inductively define a converging sequence of matrices $M_i = \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}$, such that that $M_i\rho_f(G_{\mathbf{Q}})M_i^{-1}$ consists of elements of $GL_2(\mathcal{O}_E)$ whose lower left entries are divisible by π and upper right entries are divisible by π^i. Then the limit $M = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ of the M_i's (with $lim_i t_i = t$) conjugates $\rho_f(G_{\mathbf{Q}})$ into the lower triangular subgroup of $GL_2(E)$.

The inductive hypothesis may be rephrased as: $P^iM_i\rho_f(G_{\mathbf{Q}})M_i^{-1}P^{-i}$ consists of integral matrices whose lower left corner is divisible by π^{i+1}. The reduction of this mod π is upper-triangular. As all reductions are assumed to be semisimple, and they can always be assumed to be upper triangular, there is a unipotent matrix $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ that diagonalises the reduction mod π of $P^iM_i\rho_f(G_{\mathbf{Q}})M_i^{-1}P^{-i}$. Thus $UP^iM_i\rho_f(G_{\mathbf{Q}})M_i^{-1}P^{-i}U^{-1}$ consists of matrices whose upper right corner is divisible by π while its lower left corner is still divisible by π^{i+1}. Thus $(P^{-i}UP^iM_i)\rho_f(G_{\mathbf{Q}})(P^{-i}UP^iM_i)^{-1}$ consists of integral matrices whose lower left corner is divisible by π and upper right corner entries are divisible by π^{i+1}. We can continue the induction by setting

$$M_{i+1} = P^{-i}UP^iM_i = \begin{pmatrix} 1 & t_i + \pi^i u \\ 0 & 1 \end{pmatrix},$$

and we are done after observing that conjugating by M_i does not change the order with which the characters ϕ_i appear on the diagonal.

3.2 Congruences between cuspforms and Eisenstein series

Consider the Eisenstein series

$$E_k = -B_k/2k + \Sigma_n \sigma_{k-1}(n)q^n.$$

This is a modular form for the group $SL_2(\mathbf{Z})$. We would like to prove that there is a cuspform $f \in S_k(SL_2(\mathbf{Z}))$ such that the Fourier expansion of f

has algebraic integers as coefficients and if we fix a place $\wp$ above p we have the congruence

$$a_r(f) \equiv \sigma_{k-1}(r)(\wp)$$

for almost all primes r. We may try to do this by trying to find a modular form E of weight k for $SL_2(\mathbf{Z})$ with integral Fourier coefficients such that its constant term is a unit at $\wp$, and then by considering $E_k - uB_k/2kE$, for a $\wp$-unit u, we can get a cuspform f, as $\mathcal{H}/SL_2(\mathbf{Z})$ has only one cusp. This is the procedure Ribet follows. But as Kirti Joshi has observed there is a simpler argument (a similar argument occurs in Section 2.2 of [S1]) as follows:

We consider a polynomial $f = \Sigma_{i=1}^{n} c_i \Delta^i$ for some n in the Δ function

$$\Delta := q\Pi(1-q^n)^{24} = \Sigma_{n\geq 1}\tau(n)q^n,$$

with no constant term, with coefficients $c_i = a_i E_4^{c_i} E_6^{d_i}$, with $a_i \in \mathbf{Z}$ and c_i, d_i non-negative integers, and such that $E_k - f \equiv 0 \ mod(\wp)$. Observe that the semigroup generated by $4c_i + 6d_i$, with c_i, d_i non-negative integers consists of all even integers greater than 4. We can find such a polynomial as the constant terms $-B_4/8$ and $-B_6/6$ of E_4 and E_6 are rational numbers with numerator 1, and the fact that, if a modular form of weight k on $SL_2(\mathbf{Z})$ has a sufficient number (roughly $k/12$) of its terms in its Fourier expansion divisible by p, then all its terms are divisible by p. This kind of argument also proves the Ramanujan congruence $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$ (see also [S1]).

It is also possible, as is mentioned in passing in [R], to give a more pure-thought proof of this result along the following lines. Consider the reduction mod $\wp$ of $\overline{E}_k$. Now we can consider this as a differential form on the curve X (that is the projective line, and the compactification of $\mathcal{H}/SL_2(\mathbf{Z})$ by a point at infinity as a Riemann surface) but now with mod p coefficients. Further the "differential form" $\overline{E_k(dq/q)^{\otimes \frac{k}{2}}}$ has no poles and thus gives a holomorphic $k/2$-form on X with mod p coefficients. By general results of Mazur (the q-expansion principle) it follows that $\overline{E}_k$ can be regarded as a global section of $\Omega_{/\mathbf{F}}^{\otimes(k/2)}$ where $\Omega_{/\mathbf{F}}$ is the canonical sheaf with $\mathbf{F}$ coefficients. Now consider the map

$$H^0(X, \Omega_{/\mathcal{O}_E}^{\otimes(k/2)}) \to H^0(X, \Omega_{/\mathbf{F}}^{\otimes(k/2)}).$$

It is then well-known (Section 2.1.2 of [C]), that this map is surjective, assuming that $p \geq 5$.

Theorem 5 *If $p|B_k$ (for $2 < k \leq p-3$), then there is a cuspform $f \in S_k(SL_2(\mathbf{Z}))$ whose Fourier coefficients are algebraic and $f \equiv E_k \pmod{\wp}$.*

But this is not good enough for us as Galois representations are attached to eigencuspforms rather than just cuspforms. Thus we have to prove:

Corollary 1 *If $p|B_k$ (for $2 < k \leq p-3$), then there is an eigencuspform $f \in S_k(SL_2(\mathbf{Z}))$ whose Fourier coefficients are algebraic and such that $f \equiv E_k \pmod{\wp}$.*

Proof. This is a lemma due to Deligne-Serre. We consider the space $S_k(SL_2(\mathbf{Z}), \mathcal{O}_E) = S_k(SL_2(\mathbf{Z}), \mathbf{Z}) \otimes \mathcal{O}_E$ and its mod p reduction that we denote by $S_k(SL_2(\mathbf{Z}), \mathbf{F})$. We consider the $\mathcal{O}_E$ algebra h generated by the Hecke operators T_r for r prime to p: this is commutative and has no nilpotent elements. We have to show that any mod p eigenform of the Hecke algebra in the latter space lifts to an eigenform of the characteristic 0 (for E sufficiently large). A mod p eigenform gives a homomorphism $h \to \mathbf{F}$ and that corresponds to a maximal ideal m. Consider the set of minimal prime ideals contained in m: at least one of them does not contain p, as h is reduced, and this provides the characteristic 0 lift that we are after. Alternatively as h is reduced we can apply the going-up theorem to conclude.

Corollary 2 *If $p|B_k$ (for $2 < k \leq p-3$), then there is an eigencuspform $f \in S_k(SL_2(\mathbf{Z}))$ whose Fourier coefficients are algebraic and such that $a_r(f) \equiv \sigma_{k-1}(r) mod(\wp)$ for almost all primes r.*

3.3 The representation ρ

After the work of the previous section a representation ρ with the properties (i) and (ii) of Theorem 2 follow easily. Namely consider an eigencuspform f as of the previous corollary. Then the semisimplification of the reduction of the mod $\wp$ reduction of ρ_f and the semisimple representation $\tau := 1 \oplus \chi^{k-1}$ of $G_{\mathbf{Q}}$ have the same characteristic polynomials for the Frobenius elements at almost all primes r. This together with the Cebotarev density theorem and a theorem of Brauer-Nesbitt, Theorem 4, implies that the semisimplification of the reduction of ρ_f and τ are isomorphic. This together with Theorems 1 and 3 implies that there exists a ρ with the property (ii) of Theorem 2. The property (i) follows by a general fact as f is a cuspform of level 1 and the curve X has good reduction everywhere. But the property (iii) is tricky. As noted above we have to exclude information at p when we consider the

p-adic representation attached to f. But it is exactly information at p that one needs!

Ribet does this by reducing to weight 2 and uses results of Raynaud ([Ra]) on finite flat group schemes over finite extensions of $\mathbf{Z}_p$ with ramification less than $p-1$, to conclude that ρ restricted to D leaves stable 2 distinct lines, and hence is semisimple.

Working in higher weights results of the type proven by Faltings-Jordan ([FJ]), together with results of Fontaine-Laffaille ([FL]), will allow one to deduce property (iii) in a similar manner. The crucial point is that we have the trivial Galois module as a submodule of ρ while [FL] and [FJ] imply that the trivial module is a quotient.

This completes the brief sketch of Ribet's converse to Herbrand.

REFERENCES

[C] Carayol, H., *Formes modulaires et représentations galoisiennes avec valeurs dans un anneau local complet*, in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture*, Contemp. Math. 165 (1994), American Math Soc., 213–237.

[FJ] Faltings, Gerd; Jordan, Bruce W. *Crystalline cohomology and* $\mathrm{GL}(2,\mathbf{Q})$, Israel J. Math. 90 (1995), no. 1-3, 1–66.

[FL] Fontaine, Jean-Marc; Laffaille, Guy *Construction de représentations p-adiques*, Ann. Sci. Ecole Norm. Sup. (4) 15 (1982), no. 4, 547–608.

[L] Lang, Serge, *Cyclotomic fields I and II*, Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, 121. Springer-Verlag, New York-Berlin, 1990. xviii+433 pp.

[MW] Mazur, B.; Wiles, A., *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. 76 (1984), no. 2, 179–330

[Ra] Raynaud, Michel, *Schémas en groupes de type* $(p,\cdots,p)$, Bull. Soc. Math. France 102 (1974), 241–280.

[R] Ribet, Kenneth A., *A modular construction of unramified p-extensions of* $\mathbf{Q}(\zeta_p)$, Invent. Math. 34 (1976), no. 3, 151–162.

[S] Serre, Jean-Pierre, *Abelian ℓ-adic representations and elliptic curves*, With the collaboration of Willem Kuyk and John Labute. Revised reprint of the 1968 original. Research Notes in Mathematics, 7. A K Peters, Ltd., Wellesley, MA, 1998.

[S1] Serre, Jean-Pierre, *Un interprétation des congruences relatives á la fonction τ de Ramanujan*, Oeuvres III, no. 80, 498–511, Springer Verlag, 1984.

[W] Wiles, Andrew, *Modular curves and the class group of* $\mathbf{Q}(\mu_p)$, Invent. Math. 58 (1980), no. 1, 1–35.

Chandrashekhar Khare
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road, Mumbai 400 005, India.
e-mail: shekhar@math.tifr.res.in